SECURITY ANALYSIS REPORT

HTTP Security Headers Assessment

Target URL:
https://www.instagram.com

Scan Date:
August 15, 2025 at 12:17 AM UTC

Overall Security Score:
76/100

Risk Level:
■ **Low**

Prepared by:
CyberHeaders Security

CONFIDENTIAL

This report contains sensitive security information and should be treated as confidential.
Distribution should be limited to authorized personnel only.

Table of Contents

1. Executive Summary

Assessment Overview

Our comprehensive security analysis has evaluated the HTTP security headers implementation for **https://www.instagram.com**. This automated assessment identified critical security gaps that require immediate attention to protect against common web vulnerabilities.

Key Findings:

- Overall Security Score: **76/100**
- Risk Classification: ■ **Low**
- Total Security Recommendations: **11**
- High-Priority Actions: **5**

Business Impact

The identified vulnerabilities expose your organization to potential security breaches, including cross-site scripting (XSS), clickjacking, and man-in-the-middle attacks. Immediate implementation of our recommendations will significantly strengthen your security posture and protect sensitive user data.

Next Steps

We recommend prioritizing the high-risk findings detailed in Section 3 and implementing the security recommendations in order of priority. Our team is available to assist with remediation efforts and ongoing security monitoring.

2. Priority Findings Quick Reference

The following table summarizes the highest priority security findings that require immediate attention:

Priority	Finding	Severity	Action Require
#1	Add missing security header: referrer-policy	HIGH	Immediate
#2	Add missing security header: cross-origin-embedder-policy	HIGH	Immediate
#3	CSP issue: CSP contains unsafe directive: unsafe-inline	HIGH	Immediate
#4	CSP issue: CSP contains unsafe directive: unsafe-eval	MEDIUM	Soon
#5	CSP issue: CSP missing important directive: base-uri	MEDIUM	Soon

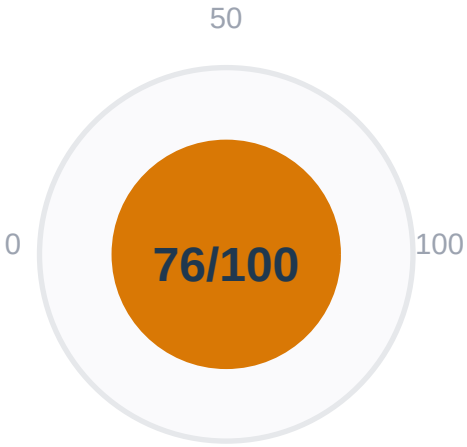
3. Scan Overview & Metrics

5.1 Scan Details

Property	Value
Target URL	https://www.instagram.com
Scan Date	August 15, 2025 at 12:17 AM UTC
Security Score	76/100
Risk Level	■ Low

Total Findings	11

5.2 Security Score Visualization

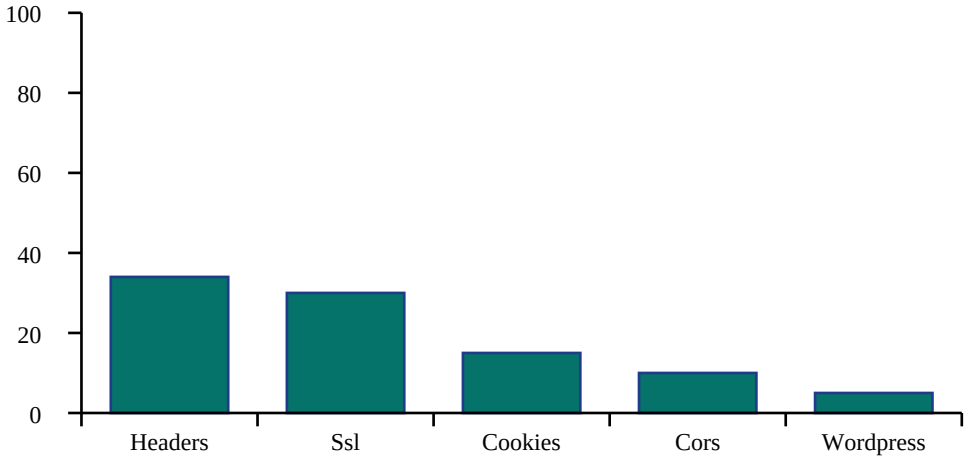


5.3 Security Category Analysis

The following analysis shows performance across different security categories:

Security Category	Score	Rating	Status
Headers	34/100	Poor	✗
Ssl	30/100	Poor	✗
Cookies	15/100	Poor	✗
Cors	10/100	Poor	✗
Wordpress	5/100	Poor	✗

Security Category Scores



4. Detailed Security Findings

6.1 Critical Missing Security Headers

The following essential security headers are missing and must be implemented immediately:

- **referrer-policy** - Critical security header not implemented

Impact: Missing referrer-policy exposes users to security vulnerabilities

Recommendation: Implement referrer-policy with appropriate security policies

- **cross-origin-embedder-policy** - Critical security header not implemented

Impact: Missing cross-origin-embedder-policy exposes users to security vulnerabilities

Recommendation: Implement cross-origin-embedder-policy with appropriate security policies

6.3 Content Security Policy Vulnerabilities

Critical Content Security Policy configuration issues:

- CSP contains unsafe directive: unsafe-inline

  Impact: CSP misconfigurations can lead to XSS vulnerabilities

- CSP contains unsafe directive: unsafe-eval

  Impact: CSP misconfigurations can lead to XSS vulnerabilities

- CSP missing important directive: base-uri

  Impact: CSP misconfigurations can lead to XSS vulnerabilities

- CSP contains overly permissive source: *

  Impact: CSP misconfigurations can lead to XSS vulnerabilities

- CSP contains overly permissive source: 'unsafe-inline'

  Impact: CSP misconfigurations can lead to XSS vulnerabilities

- CSP contains overly permissive source: data:

  Impact: CSP misconfigurations can lead to XSS vulnerabilities

5. Security Recommendations

The following recommendations are prioritized by security impact. Address high-priority items first:

1. ■ HIGH Add missing security header: referrer-policy
2. ■ HIGH Add missing security header: cross-origin-embedder-policy
3. ■ HIGH CSP issue: CSP contains unsafe directive: unsafe-inline
4. ■ HIGH CSP issue: CSP contains unsafe directive: unsafe-eval
5. ■ HIGH CSP issue: CSP missing important directive: base-uri
6. ■ MEDIUM CSP issue: CSP contains overly permissive source: *
7. ■ MEDIUM CSP issue: CSP contains overly permissive source: 'unsafe-inline'
8. ■ MEDIUM CSP issue: CSP contains overly permissive source: data:
9. ■ MEDIUM Cookie security issue: Missing HttpOnly flag
10. ■ MEDIUM Cookie security issue: Missing SameSite attribute

11. LOW Cookie security issue: Overly broad domain setting

6. Expert AI Security Analysis

Instagram Security Scan Assessment

• *1. Executive Summary:**

The security scan of Instagram (https://www.instagram.com) reveals a security score of 76/100, categorized as "Low" risk. While the site utilizes several important security headers (Strict-Transport-Security, X-Content-Type-Options, X-Frame-Options), significant vulnerabilities exist within its Content Security Policy (CSP) and cookie handling. These weaknesses, although not currently exploited, represent opportunities for attackers to inject malicious scripts and compromise user data. Immediate attention should be given to addressing the CSP and cookie security issues.

• *2. Critical Vulnerabilities:**

• **Insecure CSP:** The most critical vulnerabilities stem from the insecure configuration of the Content Security Policy (CSP). The presence of `unsafe-inline`, `unsafe-eval`, and overly permissive sources (`*`, `'unsafe-inline'`, `data:`) significantly weakens the site's protection against Cross-Site Scripting (XSS) attacks. These allow attackers to inject and execute arbitrary JavaScript code within the context of the Instagram website. The missing `base-uri` directive further increases this risk.
• **Insecure Cookies:** The absence of the `HttpOnly` and `SameSite` attributes in cookies, combined with overly broad domain settings, exposes the site to cookie theft via Cross-Site Scripting (XSS) attacks and Cross-Site Request Forgery (CSRF) attacks. This could lead to session hijacking and account compromise.

• *3. Security Header Analysis:**

• **Positive:** The presence of `Strict-Transport-Security`, `X-Content-Type-Options`, and `X-Frame-Options` headers demonstrates a commitment to basic security best practices. These headers protect against various attacks, including mixed content, clickjacking, and insecure connections.
• **Negative:** The `Content-Security-Policy` (CSP) header is poorly configured, as detailed in section 2. The missing `referrer-policy` and `cross-origin-embedder-policy` headers are also weaknesses that should be addressed. These headers help mitigate information leakage and improve cross-origin security.

• *4. WordPress-Specific Risks (if applicable):**

This section is not applicable as the scan report indicates no WordPress-related issues.

• *5. SSL/TLS Configuration Review:**

The scan indicates that SSL/TLS configuration is satisfactory. No weak cipher suites were detected, and TLS compression is disabled—all positive security indicators.

• *6. Actionable Recommendations:**

• **Prioritize CSP Remediation:** Immediately address the insecure CSP configuration. Remove `unsafe-inline`, `unsafe-eval`, `*`, `'unsafe-inline'`, and `data:` from the CSP. Implement a strict and specific CSP policy that only allows resources from trusted sources. Include the `base-uri` directive.
• **Secure Cookies:** Ensure all cookies include the `HttpOnly` and `SameSite` attributes (ideally `SameSite=Strict`). Restrict cookie domains to the strictest necessary level.
• **Add Missing Headers:** Implement the `referrer-policy` and `cross-origin-embedder-policy` headers to further enhance security.
• **Regular Security Scanning:** Implement a regular schedule for security scans to identify and address vulnerabilities proactively.
• **Penetration Testing:** Conduct periodic penetration testing to assess the effectiveness of security controls and identify potential vulnerabilities not detected by automated scans.

• *7. Overall Risk Assessment:**

While the overall score is "Low," the identified vulnerabilities in the CSP and cookie handling represent significant risks. These issues could enable attackers to gain unauthorized access to user accounts and data. The recommendations outlined above must be implemented promptly to mitigate these risks and improve the overall security posture of the Instagram website. The low score is likely influenced by the automated scanner's inability to assess the full scope of security measures implemented (e.g., WAF, server-side protections), but the identified issues should still be taken seriously.

7. Methodology & Disclaimer

Assessment Methodology

This security assessment was conducted using automated scanning techniques that analyze HTTP response headers for security configurations. Our analysis includes:

• Evaluation of essential security headers (HSTS, CSP, X-Frame-Options, etc.)
• Detection of deprecated or information-leaking headers
• Content Security Policy validation and vulnerability assessment
• SSL/TLS configuration analysis
• Cookie security evaluation
• CORS policy review

Limitations & Disclaimer

This automated assessment provides a comprehensive overview of HTTP security header implementation but does not constitute a complete security audit. For thorough security assurance, we recommend:

- Manual penetration testing
- Code review and vulnerability assessment
- Infrastructure security evaluation
- Social engineering assessments

Important Notice: This report is confidential and intended solely for the organization that requested the assessment. The findings and recommendations should be implemented by qualified security professionals.

Thank You

Thank you for choosing **CyberHeaders Security** for your security assessment needs. We are committed to helping organizations strengthen their security posture through comprehensive analysis and actionable recommendations.

This automated assessment provides valuable insights into your HTTP security headers configuration. For a more comprehensive security evaluation, we recommend conducting additional penetration testing and manual security reviews.

Contact Information

Contact Type	Details
Technical Support	Email: security@cyberheaders.com Phone: +1 (555) 123-4567
Business Inquiries	Email: sales@cyberheaders.com Phone: +1 (555) 765-4321
Website	https://www.cyberheaders.com
Address	CyberHeaders Security 123 Security Boulevard Cyber City, CC 12345 United States

Follow-up Services Available

- **Detailed penetration testing** - Comprehensive security assessment
- **Security architecture review** - Infrastructure and design analysis
- **Compliance assessments** - Regulatory compliance verification
- **Security training and awareness** - Staff education programs
- **Incident response planning** - Emergency response preparation

Contact us to discuss how we can further enhance your security posture.